网银 SSL 证书部署还有漏洞?

笔者于 **2010 年 12 月 6 日**为《计算机世界》特约撰稿发表了《**网银 SSL 证书部署有漏洞**》的技术文章，指出了当时的各大银行的网银 SSL 证书部署出现的六大安全问题。今天笔者又使用 Qualys SSL 实验室提供的 SSL 证书部署体检系统给排名前十大银行的个人网银系统做了一遍 SSL 证书部署体检，发现 11 年后的今天，各大银行的网银 SSL 证书安全部署情况仍然不容乐观，居然有两个银行打分为 **F** (按 ABCDEF 打分，最高为 A+)。

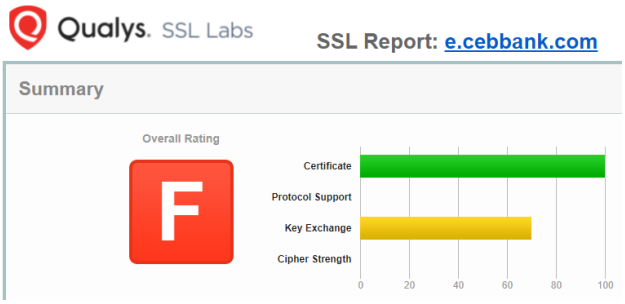
Qualys SSL 体检从 SSL 证书、协议支持、密钥交换和加密强度等 4 个维度来检测，各大银行的 SSL 证书部署安全体检得分和发现的安全问题见下表所示，下表中列出的前 6 个体检指标就是 11 年前笔者的文章中提到的必须修复的安全漏洞，很遗憾的是 11 年后仍然存在不少安全漏洞。表格中增加了一个新的检测指标：DNS CAA 支持，居然没有一个网银系统支持，这是指定某家特定 CA 为网银系统签发 SSL 证书，对保护网银系统安全非常重要，特别是网银 App 在连接网银系统时如果能验证证书是否由特定中级根证书签发，对防止 SSL 证书中间人攻击非常有用，这一点请参考笔者的另一篇博文《手机 App HTTPS 加密宝典》。

银行排名	得分	安全重新协商	关闭不安全协议	关闭不安全和弱强度加密套件	密钥长度 2048 位	全球信任	完整证书链	支持 DNS CAA
工商银行	B	支持	没有关闭 TLS 1.0/1.1	没有关闭 6 个弱强度套件	是	是	是	不支持
建设银行	B	支持	没有关闭 TLS 1.0/1.1	没有关闭 20 个弱强度套件	是	是	是	不支持
农业银行	B	支持	没有关闭 TLS 1.0/1.1	没有关闭 11 个弱强度套件，没有 1 个可用的强套件	是	是	是	不支持
中国银行	C	支持	没有关闭 SSL 3, TLS 1.0/1.1	没有关闭 4 个弱强度套件和 2 个不安全套件	是	是	是	不支持
交通银行	B	支持	没有关闭 TLS 1.0	没有关闭 5 个弱强度套件，没有 1 个可用的强套件	是	是	是	不支持
招商银行	B	支持	没有关闭 TLS 1.0/1.1	没有关闭 7 个弱强度套件，没有 1 个可用的强套件	是	是	是	不支持
浦发银行	C	支持	没有关闭 TLS 1.0/1.1	没有关闭非常不安全的 64 位对称密钥，没有关闭 3 个弱强度套件，没有 1 个可用的强套件	是	是	是	不支持
兴业银行	B	支持	没有关闭 TLS 1.0/1.1	没有关闭 22 个弱强度套件，支持 HSTS	是	是	是	不支持
民生银行	F	支持	没有关闭 SSL 3、TLS 1.0/1.1	没有关闭非常不安全的 56 位套件、匿名套件等，没有关闭 20 个弱强度套件和 3 个不安全套件	是	是	是	不支持
光大银行	F	不支持	没有关闭 TLS 1.0, Zombie POODLE 漏洞	没有关闭 5 个弱强度套件和 2 个不安全套件	是	是	否	不支持

这里再强调一下不安全的加密套件的问题，这个问题普遍存在，是体检中发现的重灾区，特别是一个银行居然还有 56 位加密套件和使用 64 位对称密钥。浏览器同服务器握手协商加密

算法理论上是优先使用高强度的加密套件和加密算法，但是如果服务器不关闭不安全的加密算法和加密套件，等于告诉攻击者服务器接受采用不安全的加密算法实现加密通信，而弱加密强度的加密很容易被破解使得 SSL 证书加密失去了加密的意义，必须关闭所有不安全的加密套件！

最后，给大家看看得分为 A+的香港汇丰银行网站体检结果截图和得分为 F 的光大银行网银网站的体检结果截图。笔者需要在这里特别声明的是：笔者不是故意要公开披露某个银行部署 SSL 证书存在的安全漏洞，这些漏洞说和不说都是摆在所有人(包括攻击者)的面前，任何人都可以使用各种安全扫描工具包括笔者使用的 Qualys SSL 体检系统来发现这些安全漏洞。



笔者希望本文能再次引起各大银行的高度关注，及时把安全漏洞堵住。也希望熟悉银行 IT 主管的朋友能把此文转发给相关银行及其他所有银行。由于时间关系，笔者并没有遍历所有银行的网银 SSL 证书部署情况，其他银行的网银系统一定也存在这些问题，真心希望通过本文和大家的共同努力能提升我国网银系统的安全水平。

王高华

2021 年 12 月 24 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。

附 1:《计算机世界》2010 年 12 月 6 日报纸版面电子版截图

计算机世界 Sina Computerworld
责任编辑：李智鹏 E-mail:li_zhipeng@ccw.com.cn 关编：刘娜娜
信息安全 CSO

网银 SSL 证书部署有漏洞

SSL 证书是解决网银系统和电子商务网站账户登录安全和账户机密信息安全的惟一可靠技术手段，但是千万不要以为部署了 SSL 证书就万事大吉，不安全的部署可能比不部署还可怕。

■ 本报特约撰稿 王高华

部署 SSL 证书是保证网银系统和电子商务网站机密信息传输安全的最有效、最安全的解决方案（因为已经标准化、所有软件都支持）。但是，用户往往最容易忽略 SSL 证书是否得到正确配置，而不安全的配置将导致安全漏洞，给重要系统带来巨大安全隐患。

根据 WoSign 最新推出的“SSL 证书免费健康体检系统”的测试结果表明：我国所有已经部署了 SSL 证书的网银系统和第三方支付系统的服务器都有不同程度的 SSL 安全配置问题（有些甚至囊括了所有已知的安全漏洞），主要涉及以下几个方面的问题：

1. 许多网银网站都没有关闭不安全的传统 SSL 通信重新协商机制，更谈不上补漏支持安全重新协商机制了。

美国信息安全专家 Marsh Ray 与 Steve Dispensa 于 2009 年 9 月份公开了他们发现的 TLS/SSL 协议的安全漏洞，攻击者可以利用这种漏洞劫持用户的浏览器，并伪装成合法用户。由于 TLS 协议中的密钥再协商功能使得验证服务器及客户机身份的一连串动作中存在前后不连贯的问题，因此给了攻击者可乘之机。不仅如此，这种漏洞还给攻击者发起 Https 攻击提供了便利，Https 协议是 Http 与 TLS 协议的集合体。

发现这一漏洞之后，两位专家很快将其报告给了网络安全产业联盟（ICASI），该联盟由微软、诺基亚、思科、IBM、英特尔和 Juniper 公司创立，同时他们还将其报告给了互联网工程任务组（IETF）以及几家开源的 SSL 项目组织。2009 年 9 月 29 日，这些团体经过讨论后决定推出一项名为 Mogul 的计划，该计划将负责修补这个漏洞，计划的首要任务是尽快推出新的协议扩展版，以修复该漏洞。

微软于 2010 年 2 月 11 日发布了第 977377 号安全公告《Microsoft 安全公告：TLS/SSL 中的漏洞可能允许欺骗》，要求用户在受影响的系统上采用禁用 TLS 和 SSL 重新协商支持的替代方法，以帮助保护连接到此类服务器的客户端，免被该漏洞所利用。同时，IETF 于 2010 年 2 月发布了新的协议扩展版 RFC 5746《Transport Layer Security (TLS) Renegotiation Indication Extension，TLS 重新协商标识扩展》。各大服务器软件厂商也纷纷推出了支持此扩展协议的补丁，微软于 2010 年 8 月 16 日发布了此漏洞的补丁《MS10-049：SChannel 中的漏洞可能允许远程代码执行》，凡是允许自动升级的系统都会自动修复此漏洞，使得系统能支持新的 TLS/SSL 协议扩展项，即支持 Secure Renegotiation（安全重新协商）。Apache 服务器软件也提供了相应的补丁。

但是，这么重大的安全漏洞并没有引起国内部署了 SSL 证书的重要系统的重视和采取相应行动。所幸的是：如果服务器采用的是 Windows Server 系统并支持自动升级的话，微软已经自动升级和修复了此安全漏洞。但还有许多服务器软件并不支持自动升级功能，特别是被广泛使用的 Apache 服务器软件，必须人工升级到最新版。

2. 有许多网站仍然支持不安全的 SSL V2.0 协议。

SSL V2.0 协议是 NetScape 公司于 1995 年 2 月发布的，由于 V2.0 版本有许多安全漏洞，所以，1996 年紧接着发布了 V3.0 版本。目前主流浏览器（IE、火狐、谷歌、Safari、Opera 等）都已经不支持不安全的 SSL V2.0 协议。SSL V2.0 协议的主要安全漏洞有：同一加密密钥用于消息身份验证和加密；弱消息认证代码结构和只支持不安全的 MD5 摘要算法；SSL 握手过程没有采取任何防护，这意味着非常容易遭遇中间人攻击；虽然使用 TCP 连接关闭，以指示数据的末尾，但并没有明确的会话关闭通知（这意味着截断攻击是可能的，攻击者只需伪造一个 TCP FIN，使得接受方无法识别数据结束消息的合法性即可）。

3. 有些网站仍然支持不安全的 40 位和 56 位加密套件。

破解 40 位 DES 算法只需几秒钟，破解 50 位 DES 算法也只需几天时间，但破解 128 位 3DES 算法则需要 0.25 个 10 的 21 次方年才能破解，所以，Web 服务器软件必须只能支持 128 位以上的加密套件，而关闭不安全的 40 位和 56 位加密套件。

4. 有些网站的 SSL 证书和/或其根证书都是不安全的 1024 位公钥。

微软和火狐等将于 2010 年 12 月 31 日停止支持 1024 位公钥证书，并于 2013 年 12 月 31 日之前删除所有不安全的、低于 2048 位的根证书。为了服务器的安全，必须部署从根证书、中级根证书和用户证书整个证书链都是 2048 位或高于 2048 位的 SSL 证书。

5. 许多网银系统都使用自签证书或其他不支持浏览器的 SSL 证书，几乎所有自签证书都存在以上安全问题，并且自签证书很容易假冒和受到中间人攻击。

为了重要系统的安全，千万不要使用自签的 SSL 证书，避免因此产生的巨大安全隐患和安全风险，特别是重要的网银系统、网上证券系统和电子商务系统，一定要选购专业证书颁发机构颁发的全球信任的支持浏览器的 SSL 证书，因为证书中许多环节的安全问题是一般的自签证书颁发系统都没有很好解决的技术问题。

6. 有些网站的 SSL 证书安装时并没有安装中级根证书。

这对于 IE 浏览器是没有问题的，但火狐浏览器访问时会有安全警告。为了让用户能正常访问部署了 SSL 证书的网站，必须正确安装中级根证书。

SSL 证书是解决网银系统和电子商务网站账户登录安全和账户机密信息安全的惟一可靠技术手段，但是千万不要以为部署了 SSL 证书就万事大吉了，不安全的部署可能比不部署还可怕，因为用户看到有安全锁标志就以为安全了，实际上却存在安全漏洞和安全隐患。望所有部署了 SSL 证书的网站都使用相关安全工具来自查，发现有哪些安全漏洞后及时联系证书销售方获得技术帮助。

附 2：《计算机世界》2010 年 12 月 6 日文章《网银 SSL 证书部署有漏洞》原文

网银 SSL 证书部署有漏洞

本报特约撰稿 王高华

SSL 证书是解决网银系统和电子商务网站账户登录安全和账户机密信息安全的唯一可靠技术手段，但是千万不要以为部署了 SSL 证书就万事大吉，不安全的部署可能比不部署还可怕。

部署 SSL 证书是保证网银系统和电子商务网站机密信息传输安全的最有效、最安全的解决方案，也是最简单的解决方案(因为已经标准化、所有软件都支持)。但是，用户往往最容易忽略 SSL 证书是否得到正确配置，而不安全的配置将导致安全漏洞，给重要系统带来巨大安全隐患。

根据 WoSign 最新推出的“SSL 证书免费健康体检系统”的测试结果表明：我国所有已经部署了 SSL 证书的网银系统和第三方支付系统的服务器都有不同程度的 SSL 安全配置问题(有些甚至囊括了所有已知的安全漏洞)，主要涉及以下几个方面的问题：

1. **许多网银网站都没有关闭不安全的传统 SSL 通信重新协商机制，更谈不上补漏支持安全重新协商机制了。**

美国信息安全专家 Marsh Ray 与 Steve Dispensa 于 2009 年 9 月份公开了他们发现的 TLS/SSL 协议的安全漏洞，攻击者可以利用这种漏洞劫持用户的浏览器，并伪装成合法用户。由于 TLS 协议中的密钥再协商功能使得验证服务器及客户机身份的一连串动作中存在前后不连贯的问题，因此给了攻击者可乘之机。不仅如此，这种漏洞还给攻击者发起 Https 攻击提供了便利，Https 协议是 Http 与 TLS 协议的集合体。

发现这一漏洞之后，两位专家很快将其报告给了网络安全产业联盟（ICASI)，该联盟由微软、诺基亚、思科、IBM、英特尔和 Juniper 公司创立，同时他们还将其报告给了互联网工程任务组（IETF）以及几家开源的 SSL 项目组织。2009 年 9 月 29 日，这些团体经过讨论后决定推出一项名为 Mogul 的计划，该计划将负责修补这个漏洞，计划的首要任务是尽快推出新的协议扩展版，以修复该漏洞。

微软于 2010 年 2 月 11 日发布了第 977377 号安全公告《Microsoft 安全公告：TLS/SSL 中的漏洞可能允许欺骗》，要求用户在受影响的系统上采用禁用 TLS 和 SSL 重新协商支持的替代方法，以帮助保护连接到此类服务器的客户端，免被该漏洞所利用。同时，

IETF 于 2010 年 2 月发布了新的协议扩展版 RFC 5746《Transport Layer Security (TLS) Renegotiation Indication Extension，TLS 重新协商标识扩展》。各大服务器软件厂商也纷纷推出了支持此扩展协议的补丁，微软于 2010 年 8 月 16 日发布了此漏洞的补丁《MS10-049：SChannel 中的漏洞可能允许远程代码执行》，凡是允许自动升级的系统都会自动修复此漏洞，使得系统能支持新的 TLS/SSL 协议扩展项，即支持 Secure Renegotiation (安全重新协商)。Apache 服务器软件也提供了相应的补丁。

但是，这么重大的安全漏洞并没有引起国内部署了 SSL 证书的重要系统的重视和采取相应行动。所幸的是：如果服务器采用的是 Windows Server 系统并支持自动升级的话，微软已经自动升级和修复了此安全漏洞。但还有许多服务器软件并不支持自动升级功能，特别是被广泛使用的 Apache 服务器软件，必须人工升级到最新版。

2. 有许多网站仍然支持不安全的 SSL V2.0 协议。

SSL V2.0 协议是 NetScape 公司于 1995 年 2 月发布的，由于 V2.0 版本有许多安全漏洞，所以，1996 年紧接着发布了 V3.0 版本。目前主流浏览器(IE、火狐、谷歌、Safari、Opera 等)都已经不支持不安全的 SSL V2.0 协议。SSL V2.0 协议的主要安全漏洞有：同一加密密钥用于消息身份验证和加密；弱消息认证代码结构和只支持不安全的 MD5 摘要算法；SSL 握手过程没有采取任何防护，这意味着非常容易遭遇中间人攻击；虽然使用 TCP 连接关闭，以指示数据的末尾，但并没有明确的会话关闭通知（这意味着截断攻击是可能的，攻击者只需伪造一个 TCP FIN，使得接受方无法识别数据结束消息的合法性即可）。

3. 有些网站仍然支持不安全的 40 位和 56 位加密套件。

破解 40 位 DES 算法只需几秒钟，破解 50 位 DES 算法也只需几天时间，但破解 128 位 3DES 算法则需要 0.25 个 10 的 21 次方年才能破解，所以，Web 服务器软件必须只能支持 128 位以上的加密套件，而关闭不安全的 40 位和 56 位加密套件。

4. 有些网站的 SSL 证书和/或其根证书都是不安全的 1024 位公钥。

微软和火狐等将于 2010 年 12 月 31 日停止支持 1024 位公钥證书，并于 2013 年 12 月 31 日之前删除所有不安全的、低于 2048 位的根证书。为了服务器的安全，必须部署从根证书、中级根证书和用户证书整个证书链都是 2048 位或高于 2048 位的 SSL 证书。

5. **许多网银系统都使用自签证书或其他不支持浏览器的 SSL 证书，**几乎所有自签证书都存在以上安全问题，并且自签证书很容易假冒和受到中间人攻击。

为了重要系统的安全，千万不要使用自签的 SSL 证书，避免因此产生的巨大安全隐患和安全风险，特别是重要的网银系统、网上证券系统和电子商务系统，一定要选购专业证书颁

发机构颁发的全球信任的支持浏览器的 SSL 证书，因为证书中许多环节的安全问题是一般的自签证书颁发系统都没有很好解决的技术问题。

6. 有些网站的 SSL 证书安装时并没有安装中级根证书。

这对于 IE 浏览器是没有问题的，但火狐浏览器访问时会有安全警告。为了让用户能正常访问部署了 SSL 证书的网站，必须正确安装中级根证书。

SSL 证书是解决网银系统和电子商务网站账户登录安全和账户机密信息安全的惟一可靠技术手段，但是千万不要以为部署了 SSL 证书就万事大吉了，不安全的部署可能比不部署还可怕，因为用户看到有安全锁标志就以为安全了，实际上却存在安全漏洞和安全隐患。望所有部署了 SSL 证书的网站都使用相关安全工具来自查，发现有哪些安全漏洞后及时联系证书销售方获得技术帮助。